

Patent  
Attorney's Docket No. 032326-168

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	
Jean-Sébastien CORON	)	Group Art Unit: Unassigned
Application No.: Unassigned	)	Examiner: Unassigned
Filed: September 26, 2001	)	
For: COUNTERMEASURE METHOD IN AN	)	
ELECTRIC COMPONENT	)	
IMPLEMENTING AN ELLIPTICAL	)	
CURVE TYPE PUBLIC KEY	)	
CRYPTOGRAPHY ALGORITHM	)	

**INFORMATION DISCLOSURE STATEMENT**  
**TRANSMITTAL LETTER**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

Enclosed is an Information Disclosure Statement and accompanying form PTO-1449 for the above-identified patent application.


- ☒ [X] No additional fee for submission of an IDS is required.
- ☐ [ ] The fee of \$180.00 (126) as set forth in 37 C.F.R. § 1.17(p) is also enclosed.
- ☐ [ ] A certification under 37 C.F.R. § 1.97(e) is also enclosed.
- ☐ [ ] A certification under 37 C.F.R. § 1.97(e), and the fee of \$180.00 (126) as set forth in 37 C.F.R. § 1.17(p) are also enclosed.
- ☐ [ ] Charge \$\_\_\_\_\_ to Deposit Account No. 02-4800 for the fee due.
- ☐ [ ] A check in the amount of \$\_\_\_\_\_ is enclosed for the fee due.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800. This paper is submitted in duplicate.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620

By:   
James A. LaBarre  
Registration No. 28,632

Date: September 26, 2001

Patent  
Attorney's Docket No. 032326-168

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	
	)	
Jean-Sébastien CORON	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: September 26, 2001	)	
	)	
For: COUNTERMEASURE METHOD IN AN	)	
ELECTRIC COMPONENT	)	
IMPLEMENTING AN ELLIPTICAL	)	
CURVE TYPE PUBLIC KEY	)	
CRYPTOGRAPHY ALGORITHM	)	

**INFORMATION DISCLOSURE STATEMENT**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. §1.56, Applicants hereby submit the following information in conformance with 37 C.F.R. §§ 1.97 and 1.98. A copy of the document cited below is enclosed.

**Other Documents**

Koblitz, Neal, *"Elliptic Curve Cryptosystems"*, Mathematics of Computation, January 1987, Vol. 48, No. 177, pps. 203-209.

Kocher, Paul, *"Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems"*, Advances In Cryptology, Crypto '96, Santa Barbara, Ca, USA, August 18-22, 1996, pps. 104-113.

Kocher, Paul et al, *"Introduction to Differential Power Analysis and Related Attacks"*, Cryptography Research, Inc., February 24, 2000, pps.1-8.

Menkus, Belden, *Two Important Data Encryption Structures Reported Broken in Record Times*", EDPACS, January 1999, Auerbach Publications, Vol. 26, No. 7, pps. 15-18.

These references were cited in an International Search Report for the corresponding PCT application. A copy of that Search Report is also being submitted herewith.

To assist the Examiner, the references are listed on the attached form PTO-1449. It is respectfully requested that an initialled copy of this form be returned to the undersigned.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: September 26, 2001

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620

By:



James A. LaBarre  
Registration No. 28,632

Substitute for form 1449A/PTO  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	ATTORNEY'S DKT NO. 032326-16	APPLICATION NO. Unassigned
	APPLICANT Jean-Sébastien CORON	
	FILING DATE September 21, 2001	GROUP Unassigned

U.S. PATENT DOCUMENTS						
Examiner Initials	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication (MM-DD-YYYY)		
	Number	Kind Code (if known)				

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Foreign Patent Document		Country	Date of Publication (MM-DD-YYYY)	Translation	
	Number	Kind Code (if known)			Yes	no

NON PATENT LITERATURE DOCUMENTS	
Examiner Initials	Include name of author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	Koblitz, Neal, <i>"Elliptic Curve Cryptosystems"</i> , Mathematics of Computation, January 1987, Vol. 48, No. 177, pps. 203-209.
	Kocher, Paul, <i>"Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems"</i> , Advances In Cryptology, Crypto '96, Santa Barbara, Ca, USA, August 18-22, 1996, pps. 104-113.
	Kocher, Paul et al, <i>"Introduction to Differential Power Analysis and Related Attacks"</i> , Cryptography Research, Inc., February 24, 2000, pps.1-8.
	Menkus, Belden, <i>Two Important Data Encryption Structures Reported Broken in Record Times"</i> , EDPACS, January 1999, Auerbach Publications, Vol. 26, No. 7, pps. 15-18.

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--